Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Please amend claims 1, 3, 5, and 10 as follows:

1. (currently amended): A portable terminal for encrypting information, the portable terminal comprising:

a display for displaying financial transaction options;

an input for receiving financial data for a financial transaction;

means for generating a new key for ~~each~~the financial transaction, wherein the new key is generated using one or more variable properties of the portable terminal; and

means for encrypting the financial data with the new key.

2. (original): A portable terminal according to claim 1, wherein the new key is generated when the transaction is executed.

3. (currently amended): A portable terminal according to claim 1, wherein the one or more variable properties of the portable terminal include ~~the~~ date and time settings.

4. (original): A terminal according to claim 1, further comprising means for generating a unique challenge in addition to the new key so that a unique challenge can be issued

for each transaction.

5. (currently amended): A method of encrypting information ~~in~~by a portable terminal, the method comprising the steps of:

inputting financial data for a financial transaction at the portable terminal;

using one or more properties of the portable terminal to obtain a sequence of values for the financial transaction; ~~and~~

generating a new key based on the sequence of values for the financial transaction; and

encrypting information related to the prepared financial transaction with the new key by the portable terminal;.

A3

6. (original): A method according to claim 5, further comprising the step of:

generating a unique challenge value based on the sequence of values.

7. (original): A method according to claim 5, further comprising the steps of:

encrypting the new key and the challenge value using a public key issued by a host; and

transmitting the encrypted new key and challenge value to the host.

8. (original): A method of communicating encrypted information between a portable terminal and a self-service terminal, the method comprising the steps of:

using one or more properties of the portable terminal to obtain a sequence of values;

generating a new key based on the sequence of values;

generating a challenge value based on the sequence of values;

encrypting the new key and the challenge value using a public key; and

transmitting the encrypted key and challenge value to the self-service terminal.

9. (original): A method according to claim 8, further comprising the steps of:

A3

generating a new challenge value at the self-service terminal;

encrypting the generated challenge value using the new key;

transmitting the encrypted challenge value to the portable terminal; and

awaiting a correct response to the transmitted challenge value being transmitted by the portable terminal before accepting any subsequent transaction at the self-service terminal.

10. (currently amended): A transaction system comprising:

a self-service terminal; and

a portable terminal to execute an encryption program which is operable to use one or more variable properties of the portable terminal for ~~(i)~~ obtaining a sequence of values, and ~~(ii)~~ for generating a new key based on the sequence of values~~;~~,

the portable terminal encrypting information for a financial transaction with the new key, and the portable terminal wirelessly transmitting encrypted information to the self service terminal.

~~and~~

~~means for enabling the portable terminal and the self-service terminal to intercommunicate using the new key.~~

11. (original): A method of determining if a self-service terminal is an authentic terminal, the method comprising the steps of:

using one or more properties of a portable terminal to obtain a sequence of values;

generating a new key based on the sequence of values;

generating a challenge value based on the sequence of values;

encrypting the new key and challenge value using a public key provided by an institution;

transmitting the encrypted key and challenge to the self-service terminal;

receiving a response from the self-service terminal, decrypting the response using the new key; and

halting any further transmission unless the decrypted response includes a correct reply to the challenge value.

Please add new claims 12-23 as follows:

12. (new): The portable terminal of claim 1 wherein the one or more variable properties includes data stored in a dynamic heap of a memory.

13. (new): A portable terminal for encrypting information, the portable terminal comprising:

a user interface having a display, the display displaying transaction options for a financial transaction, the user interface receiving financial transaction data for the financial transaction;

a memory storing an encryption program;

a controller executing the encryption program to generate a key for the financial transaction, wherein the key is generated using one or more properties of the portable terminal, the controller encrypting the financial data with the key; and

a communication port, in response to the user interface executing the financial transaction, the communication port wirelessly transmitting the encrypted information.

A4

14. (new): The portable terminal of claim 13 wherein the portable terminal is a personal digital assistant (PDA) and the encrypted information is transmitted to an automated teller machine(ATM).

15. (new): The portable terminal of claim 13 wherein the key is a symmetric key.

16. (new): The portable terminal of claim 13 wherein the user interface is a keypad and the financial transaction data includes a personal identification number.

17. (new): The portable terminal of claim 16 wherein the personal identification number is biometric based.

18. (new): The portable terminal of claim 13 wherein the one or more properties include usage history stored in the memory.

A4

19. (new): The method of claim 5 further comprising:

receiving a public key issued by a host computer, wherein the encrypting information step further comprises encrypting information using the public key.

20. (new): The method of claim 8 wherein the step of generating a new key based on the sequence of values further comprises:

splitting a hash value into a first half and a second half; and

encrypting the second half with the first half to produce the new key.